Analysis of the effects of imperfections in an optical heterodyne quantum random-number generator

Analysis of the effects of imperfections in an optical heterodyne quantum random-number generator

Ugo Zanforlin,* Ross J. Donaldson, Robert J. Collins, and Gerald S. Buller
SUPA, Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University, David Brewster Building, Gait 2, Edinburgh EH14 4AS, United Kingdom

(Received 23 December 2018; published 6 May 2019)

Quantum random numbers generators (QRNGs) rely on quantum systems to produce sequences of random numbers with an overall lower level of predictability than classical algorithmic systems. Over the past two decades, phase randomizations of coherent sources from quantum spontaneous emission effects have gained a lot of interest due to their operational simplicity, cost-contained components, and ability to generate random numbers at high rates. However, many QRNGs require optimal calibration and alignment to ensure efficient and effective random-number generation. This work demonstrates a detailed analysis of a heterodyne measurement based QRNG, which implements phase randomization from two independent laser sources. The analysis also quantifies the effects of setup misalignments using the Kullback-Leibler divergence as a benchmark to assess the limiting conditions of secure random-number generation.

DOI: 10.1103/PhysRevA.99.052305

I. INTRODUCTION

A requirement for randomness is present in many modern technologies, e.g., digital security, numerical simulations, and electronic gambling [1,2]. The random numbers used in these applications must be uniformly distributed and truly independent from each other [3], otherwise the security of these digital systems could be compromised [4,5]. Classical algorithmic random-number generators are commonly used to produce random numbers, given the relative simplicity and low cost with which they can be implemented, and their comparatively fast data generation rates [6,7]. However, such generators only produce numbers which appear random when analyzed using a system with limited computational power and resources.

On the contrary, quantum random-number generators (QRNGs) have a level of randomness which relies on the intrinsic probabilistic nature of quantum measurements dictated by quantum mechanics [8]. There is broad range of phenomena which can be exploited for QRNGs, for example, single-photon detection [9–14], amplified spontaneous emission noise [15,16], vacuum fluctuations [17–22], and photon number distributions [23–26]. Commercial devices, which utilize QRNGs, already exist [27], however, the generation rates are in the low $\mathrm{Mb\,s^{-1}}$ range. For applications in, for example, quantum key distribution [28–30] or quantum digital signatures [31,32], which consume random numbers in the $\mathrm{Gb\,s^{-1}}$ regime, higher QRNG rates are required. QRNGs that employ quantum phase noise from spontaneous emission of a laser source offer advantages in terms of generation rate, operational simplicity, and the potential to be implemented using low cost components.

In this paper, we present a practical implementation of an optical QRNG using the phase noise between two independent laser sources operated in continuous wave (cw) mode at telecommunication wavelength (1550 nm) to provide compatibility with off-the-shelf commercial components. The system makes use of heterodyne detection of coherent states and we experimentally demonstrate a high secure postprocessed offline generation rate of $110\ \mathrm{Gb\,s^{-1}}$ and a real-time extraction rate of $15\ \mathrm{Mb\,s^{-1}}$. We also quantify the degree of interference by an external eavesdropper in the generation process, which inevitably lowers both the security and bit rate of the random numbers.

II. METHODS

A. Heterodyne measurement

Heterodyne systems retrieve phase and frequency modulations by downmixing two different optical oscillators, i.e., a local oscillator (LO) and a signal (SG) [33]. The LO is used as a reference source to which the SG is compared and the resulting output signal is measured by a detector which exhibits a linear electrical response to linear changes in incident optical energy [34]. Quantum mechanically, the light produced by a laser source can be described in terms of coherent states [35], however, it is possible to reduce the analysis to a semiclassical electromagnetic fields system while still retaining the same amount of information [36]. Under this framework, when the electric fields associated with the LO (E_{LO}) and SG (E_{SG}) interfere, the resulting superposition field E_{D} reaching the detector becomes

$$E_{\mathrm{D}}(t) = E_{\mathrm{LO}}\ \cos\left(\omega_{\mathrm{LO}}\, t + \phi_{\mathrm{LO}}\right) + E_{\mathrm{SG}}\ \cos\left(\omega_{\mathrm{SG}}\, t + \phi_{\mathrm{SG}}\right), \tag{1}$$

where ω_{LO} and ω_{SG} are the optical frequencies of the LO and the SG respectively, and ϕ_{LO} and ϕ_{SG} are the optical phases mainly arising from spontaneous emission of the laser sources. Our system comprises polarization maintaining optical fibers allowing us to assume that the polarization modes of the two fields are the same and are both linear. The superposition of the electrical fields is a linear operation

*uz2@hw.ac.uk

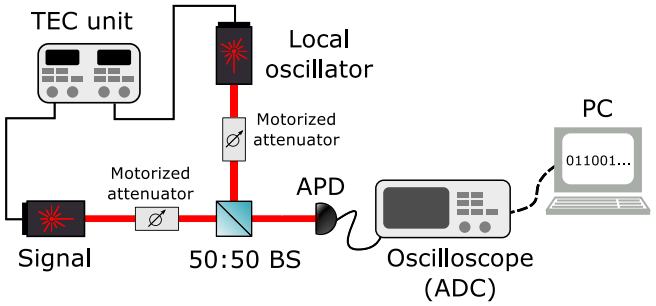

FIG. 1. Experimental setup of the heterodyne quantum random-number generator (QRNG). Two independent DFB lasers ($\lambda \approx 1550$ nm), operated in continuous-wave mode and controlled by a driving current and TEC unit, interfere at a 50:50 beam splitter (BS). The random interference output is registered by a fast InGaAs/InP APD which is monitored by a 12-bit resolution ADC connected to a computer for postprocessing and randomness extraction.

where the resulting interference depends on the relative phase difference between the fields themselves [33]. The detectors output I_D can be shown to follow the dependence:

$$I_D \propto \sqrt{I_{LO}}\sqrt{I_{SG}}\,\cos(\Delta\omega\, t + \Delta\phi), \tag{2}$$

where $\Delta\omega$ and $\Delta\phi$ define the differences between the angular frequencies and optical phases of the LO and the SG respectively while I_{LO} and I_{SG} are the electrical intensities of the LO and the SG respectively. As long as the phases of both the LO and SG are dominated by spontaneous emission, $\Delta\phi$ is uniformly distributed in the range $[0, 2\pi]$. In our experiment we show the probability distribution arising from the heterodyne detection of two coherent states interference and how it is affected by adjusting $\Delta\omega$, related to the central wavelength mismatch between the two laser sources, and I_{LO} and I_{SG}.

B. Experimental method

The experimental heterodyne system is shown in Fig. 1. Both the LO and the SG are tunable narrow band distributed feedback (DFB) lasers with 1-GHz linewidth close to 1550-nm peak wavelength. A thermoelectric cooler (TEC) unit allows wavelength tuning of both lasers, which directly affects $\Delta\omega$. The TEC unit had a temperature stability of $\pm 0.01\,^{\circ}$C corresponding to a measured $\sim$1.51-pm shift in central wavelength. Both the LO and the SG emit light in a continuous wave (cw) mode and can be treated as two independent sources producing two laser beams of random relative phase ($\Delta\phi$). Working with cw emission eliminates the requirement for precise matching of the interferometric optical path lengths, which other QRNGs operating via phase noise require [37,38]. The intensities of both lasers are finely tunable via two motorized variable optical attenuators (MVOAs) with 0.1-dB resolution. Both lasers include an internal monitoring photodiode which serves to limit the optical power fluctuations at the sources to $\sim 3 \times 10^{-8}\%$ of the operational output power, thereby limiting degradation of the interferometric visibility caused by power fluctuations. The operational optical powers of both sources matched at the BS using motorized attenuators ($P_{LO} = 1.26$ mW and $P_{SG} = 1.28$ mW) have been chosen to maximize the contribution of spontaneous emission over stimulated emission for optimal randomness extraction (see Appendix B for the detailed analysis). The optical power levels showed a 1.5% mismatch, however, no visibility degradation was detected due to the higher contribution of the detector's noise to the overall signal. Moreover, the chosen optical power levels broaden the spectral linewidths $\sim$0.0211 nm of both sources allowing higher sampling rate ($\sim$10 GHz) while retaining uniformity and independence in $\Delta\phi$ [39]. The outputs of the LO and the SG are interfered at a 50:50 beam splitter which is in turn connected to a balanced receiver [InGaAs/InP avalanche photodiode (APD); 25-GHz bandwidth, 18.5-ps rise time], the electrical output of which is read by a fast high-resolution digital oscilloscope [20-GHz bandwidth, 12-bit resolution analog-to-digital converter (ADC)] which served to convert the analog signal from the APD into a digital signal for postprocessing and randomness extraction. All optical components are fiber coupled using single mode panda-eye polarization-maintaining fiber [40] to limit interference visibility degradation. The interferometer was kept in mechanical isolation and in a temperature controlled environment with a $\pm 0.15\,^{\circ}$C stability. Carefully matching the optical power of both the LO and the SG using the individual MVOAs and driving current, as well as their wavelengths via temperature tuning with the TEC unit, granted optimal randomness generation. Wavelength matching not only plays a major role in achieving high quality interference and therefore randomness generation but also defines the beat frequency $\Delta\omega$ of the heterodyne measurement, i.e., the smaller the $\Delta\omega$, the less correlation is present in the extraction process for a given sampling rate. The beat frequency $\Delta\omega$ is related to the wavelengths λ_{LO} and λ_{SG} of the LO and SG respectively as $\Delta\omega = (\frac{c}{n})2\pi|\frac{1}{\lambda_{SG}} - \frac{1}{\lambda_{LO}}|$ where c is the speed of light in vacuum and n is the refractive index of the medium through which LO and SG propagate. The system's receiver was balanced by digitally selecting a frequency extraction window, i.e., 10 GHz centered at 7.6 GHz, where the detector's electrical response was uniform in order to reduce classical noise introduced by device imperfections. The digital signal produced by the fast oscilloscope was then postprocessed using custom analysis routines written in MATLAB [41], which computed and assessed the security and performance of the system. Standard NIST 800-22 [42] and DIEHARDER [43] testing suites were then used to provide a preliminary assessment of the randomness of the generated numbers. Further tests must be conducted on the output of the QRNG to verify that it is not unduly correlated with the environment and these are considered in subsequent sections for our QRNG.

III. EXPERIMENTAL RESULTS

A. Probability distribution and information entropy

Figure 2 shows the probability distributions for a single coherent state, i.e., when LO and SG are active without interfering [Figs. 2(a) and 2(b)], the electric noise of the detector [Fig. 2(c)], and two coherent states interference, i.e., when both LO and SG laser sources are active [Fig. 2(d)]. The probability distribution of the two coherent states' interference

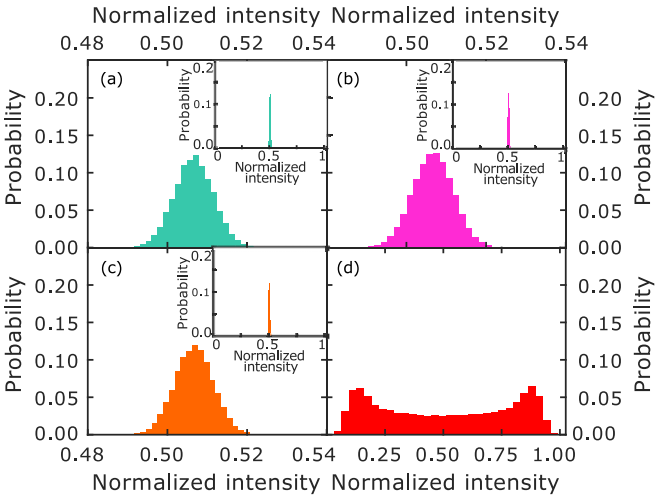

FIG. 2. Probability distributions of (a) local oscillator (LO), (b) signal (SG), (c) electrical background from the APD detector, and (d) quantum interference when the LO and SG are indistinguishable.

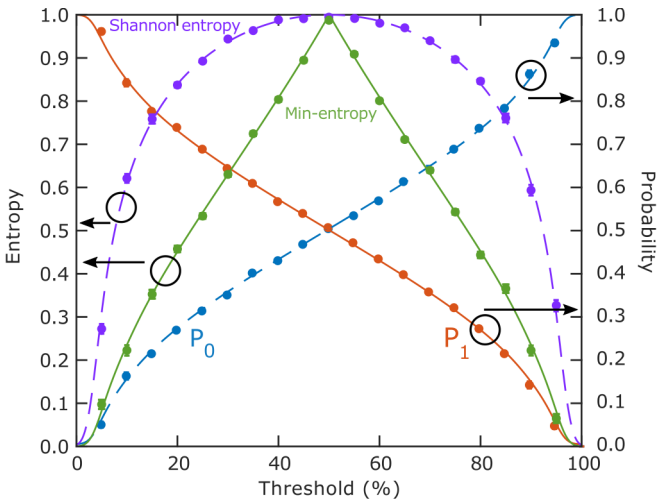

FIG. 3. Shannon entropy (dashed purple line), min-entropy (solid green line), and binary probability distributions, i.e., P_0 (dashed blue line) and P_1 (solid orange line) as a function of the extraction threshold level. In our case, the achievable maximum entropy is 0.967 bit^{-1} at a threshold level of 49.95%. Error bars of experimental values are less than 5% and covered by the plot symbols.

follows an arcsine distribution as the randomized phase difference $\Delta\phi$ between the laser sources is uniformly distributed in the range $\Delta\phi \in [0, 2\pi]$. Such a distribution is easily discernible from the others shown in Figs. 2(a)–2(c) as they follow a Gaussian profile as predicted by the central limit theorem [44]. Probability distribution analysis provides a first assessment on the underlying physical process of a QRNG, however, it is also important to quantify the amount of nonredundant information that can be extracted from the pool of data samples. In information theory, the family of Rényi entropies are the mathematical tools that allow quantifying the degree of information associated with a random variable [45,46]. The two most commonly used entropies are the Shannon entropy and min-entropy [47–49]. To study the amount of entropy found in the system we implement a threshold level extraction mechanism, i.e., a value stored by the ADC is converted into either a binary 1 or 0 if it is higher (lower) than a specific voltage value, binary probability distributions are then computed and used to estimate both entropies. Figure 3 shows both Shannon and min-entropy as a function of the threshold level as well as the associated binary distributions. The threshold is selected to ensure that the output sequence of random binary digits is balanced to have equal numbers of 1's and 0's when considered over a sequence of prestored 10^6 bit string. In our case, both entropies were maximized at 0.967 bit^{-1} for a threshold level of 49.95% showing great agreement with the expected theoretical value of 50% for a balanced system. As soon as the threshold moves from that optimal position, an asymmetry in the probabilities arises and the amount of nonredundant extractable information diminishes reaching a minimum level at both extremes (see Fig. 3). Our entropy estimation and binary probability distribution analysis do not take into account limiting factors, e.g., detector's discretization effects and side information correlations, as the required extra analysis goes beyond the scope of this work.

B. Security analysis

Despite having maximized entropy and showing ideal arcsine probability distribution, the system might be correlated with the environment or an eavesdropper or malicious party could control part of the device. Our QRNG depends on the interference of two independent coherent states, and of all the parameters that influence the visibility of the interferometer, e.g., polarization, temperature, mechanical stress, etc., affect the output of the system; Eq. (2) shows that the intensity registered by the detector is proportional to the product of the square root of the LO and SG intensities and that it is also affected by the wavelength difference, $\Delta\omega$, between the LO and SG. However, in randomness generation the aim is to calibrate the LO and the SG to be highly indistinguishable and to maximize the uncertainty in the measurements, therefore there is a limit to how distinguishable the two signals can be which is not incorporated in the theoretical formulation. The absolute beat frequency $\Delta\omega$ can be expressed as the sum of two independent terms, i.e., $\Delta\omega = \Delta\omega_{\mathrm{I}} + \Delta\omega_{\mathrm{T}}$. $\Delta\omega_{\mathrm{I}}$ is the induced beat frequency from experimental limitations in wavelength matching due to the finite temperature resolution of the TEC unit when optimal quantum interference is measured, in our case $\Delta\omega_{\mathrm{I}} \approx 188$ MHz. $\Delta\omega_{\mathrm{T}}$ is the measured beat frequency when the temperature of the LO and SG are actively changed via the TEC unit. Figure 4 shows the time evolution of the probability distribution as $\Delta\omega$ increases while Fig. 5 shows the time evolution of the probability distribution as the difference of the optical powers of the LO and the SG, i.e., $\Delta I = |I_{\mathrm{LO}} - I_{\mathrm{SG}}|$, increases. The optimal ΔI value is set to 500 nW, the smallest possible intensity variation due to the stabilization feedback control of the DFB lasers, while the maximum value of 2.5 mW is achieved by increasing the operational power up to ~2.5 mW. As can be seen from Fig. 4, the distribution transitions from an arcsine to a Gaussian as $\Delta\omega$ increases. As the separation between the two wavelengths increases, the beat frequency $\Delta\omega$ increases until the time-averaging sampling of the detector dominates

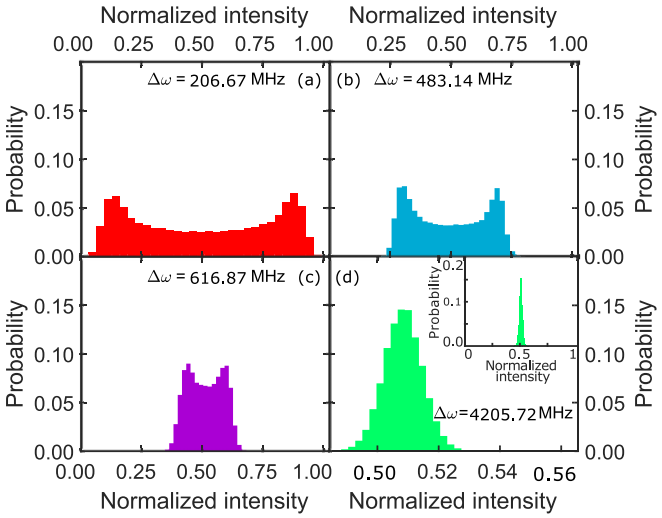

FIG. 4. Evolution of the probability distribution for different values of $\Delta\omega$. When LO and SG are indistinguishable, the quantum interference takes place and the arcsine is retrieved (a). As the wavelength's difference $\Delta\omega$ increases, the full width at half maximum of the arcsine distribution reduces, drawing the two sideband peaks together [see (b) and (c)], until the distribution transforms into a Gaussian distribution (d). All distributions have been acquired with optimal intensity matching, $\Delta I \approx 500$ nW.

the signals envelope, flattening the electrical response. In addition, when the two angular frequencies ω_{LO} and ω_{SG} are spectrally separated by more than 4 GHz, the two coherent states no longer downmix and can be considered to be in two distinguishable separate spectral modes, thereby precluding interference at the BS. Due to the intrinsic electrical noise

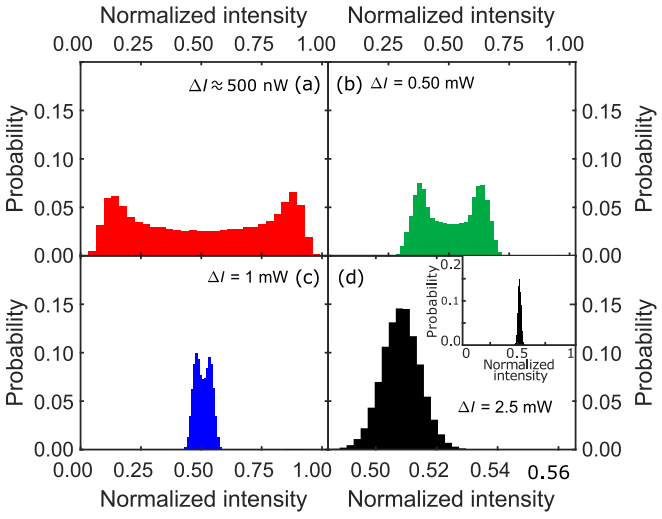

FIG. 5. Evolution of the probability distribution for different values of ΔI. When the intensities of both LO and SG are identical, the quantum interference takes place and the arcsine is retrieved (a). As the intensities difference ΔI increases, the full width at half maximum of the arcsine distribution reduces, drawing the two sideband peaks together [see (b) and (c)], until the distribution transforms into a Gaussian distribution (d). All distributions have been acquired with optimal wavelength matching, $\Delta\omega = 206.67$ MHz.

of the detector, the final distribution broadens and assumes the characteristic Gaussian shape. All $\Delta\omega$ values are defined relative to the condition of optimal quantum interference [Fig. 4(a)] which is set to $\Delta\omega = 206.67$ MHz as reference. Similarly, in Fig. 5, as ΔI increases, the distribution follows the same evolution since the difference between the mean photon numbers $|\alpha|^2$ and $|\beta|^2$, associated with the coherent state $|\alpha\rangle$ of the LO and $|\beta\rangle$ of the SG, becomes big enough to suppress the contribution of the interference letting the convolution of the individual lasers emerge. Notably, the distribution loses its characteristic arcsine shape only for high ΔI values, i.e., ~2.5 mW, corresponding to a divergence of more than three orders of magnitude from the optimal case $\Delta I \approx 500$ nW. Wavelength mismatch, on the other hand, shows the appearance of a Gaussian distribution [Fig. 4(d)] when $\Delta\omega$ diverges from the optimal case $\Delta\omega = 206.67$ MHz by just 20 times, showing that the system is more robust against intensity fluctuations in the LO and the SG than wavelength misalignments.

This analysis shows that, when the system is not optimally calibrated, the randomness generated by the interference of the two lasers is highly suppressed. Therefore, the user has the ability to monitor the generation process and detect if the system is being controlled or manipulated by an eavesdropper, or there are malfunctions during the operational lifetime.

C. Randomness distillation and testing

The probability distribution that arises from the interference of two independent laser sources is described by an arcsine function (see Sec. III A), which inevitably affects the generated random numbers, i.e., they are not uniformly distributed. Therefore, it is imperative to process further the raw samples to reduce correlations and side information. Privacy amplification, in the framework of universal hashing functions, is able to distill high quality random numbers from biased random sequences at the expense of a lower bit rate [50]. In our experiment, we made use of the Toeplitz matrix hashing technique (see Appendix D) providing information theoretic security [51]. The Toeplitz matrix construction considers the data size, min-entropy estimation, and security level [52]. The hashing extraction allows us to produce secure random numbers with a generation rate of 110 Gb s^{-1} making use of a 4096×3960 Toeplitz matrix. A prestored set of random numbers have been tested using the widely implemented NIST SP 800-22 and DIEHARDER suites to provide a preliminary assessment of the generated randomness. The complete results of the randomness tests have been included in Appendix A. When our QRNG system is not optimally calibrated, or an eavesdropper is actively interfering, the generation process is affected and the resulting distribution changes from an arcsine to a Gaussian function (see Sec. III B) which sequentially introduces more correlations in the random numbers. Referencing Tables I and II from Appendix A, when the system is optimally aligned, i.e., $\Delta\omega = 206.67$ MHz, the generated numbers pass all tests, however, as $\Delta\omega$ increases, we see an increasing number of tests failing. These results clearly confirm the requirement for calibration and monitoring of the optical setup to limit the amount of correlations that are introduced by the detector. In addition to the statistical tests,

TABLE I. NIST SP 800-22 tests results. A test is successful if the p-value satisfies the condition p-value $\geqslant \alpha$, where α is the chosen level of significance.

	NIST SP 800-22					
	$\Delta\omega = 206.67$ MHz		$\Delta\omega = 616.87$ MHz		$\Delta\omega = 4205.72$ MHz	
TEST	p-value	Result	p-value	Result	p-value	Result
Frequency	0.964295	PASSED	0.888137	PASSED	0.001084	FAILED
Block frequency	0.046169	PASSED	0.195163	PASSED	0.006990	FAILED
Cumulative sums	0.422034	PASSED	0.689019	PASSED	0.007422	FAILED
Runs	0.155209	PASSED	0.619772	PASSED	0.007880	FAILED
Longest run	0.739918	PASSED	0.378138	PASSED	0.009936	FAILED
Rank	0.378138	PASSED	0.002869	FAILED	0.004573	FAILED
FFT	0.723129	PASSED	0.002126	FAILED	0.002126	FAILED
Nonoverlapping template	0.060239	PASSED	0.000142	FAILED	0.002316	FAILED
Overlapping template	0.551026	PASSED	0.008774	FAILED	0.001346	FAILED
Universal	0.500934	PASSED	0.264458	PASSED	0.006990	FAILED
Approximate entropy	0.287306	PASSED	0.378138	PASSED	0.007422	FAILED
Random excursions	0.340461	PASSED	0.004784	FAILED	0.169178	PASSED
Random excursions variant	0.146359	PASSED	0.003699	FAILED	0.132858	PASSED
Serial	0.311542	PASSED	0.204076	PASSED	0.000316	FAILED
Linear complexity	0.186566	PASSED	0.001125	FAILED	0.000247	FAILED

we evaluated the autocorrelation coefficient K of prestored 128-Mb strings for different $\Delta\omega$ values at a fixed sampling rate of 10 GHz whose results are reported in Appendix C. The computed K-values corroborate our previous analysis and results where high randomness was only achievable when the two laser sources were indistinguishable while also proving

TABLE II. DIEHARDER tests results. A test is successful if the p-value satisfies $0.01 \leqslant p\text{-value} \leqslant 0.99$.

	DIEHARDER					
	$\Delta\omega = 206.67$ MHz		$\Delta\omega = 616.87$ MHz		$\Delta\omega = 4205.72$ MHz	
TEST	p-value	Result	p-value	Result	p-value	Result
diehard birthdays	0.120192	PASSED	0.365844	PASSED	0.903437	PASSED
diehard operm5	0.193108	PASSED	0.124769	PASSED	0.993316	PASSED
diehard rank 32x32	0.849925	PASSED	0.036587	PASSED	0.000000	FAILED
diehard rank 6x8	0.034400	PASSED	0.000000	FAILED	0.130760	PASSED
diehard bitstream	0.984981	PASSED	0.000000	FAILED	0.000000	FAILED
diehard opso	0.451348	PASSED	0.982457	PASSED	0.018327	PASSED
diehard oqso	0.469156	PASSED	0.289625	PASSED	0.000000	FAILED
diehard DNA	0.526109	PASSED	0.000000	FAILED	0.000000	FAILED
diehard count 1s str	0.468670	PASSED	0.496325	PASSED	0.000000	FAILED
diehard count 1s byte	0.584186	PASSED	0.886326	PASSED	0.000000	FAILED
diehard parking lot	0.166806	PASSED	0.000000	FAILED	0.000000	FAILED
diehard 2dsphere	0.818299	PASSED	0.000000	FAILED	0.335782	PASSED
diehard 3dsphere	0.616278	PASSED	0.069852	PASSED	0.155917	PASSED
diehard squeeze	0.744275	PASSED	0.328914	PASSED	0.000000	FAILED
diehard sums	0.036712	PASSED	0.000000	FAILED	0.000000	FAILED
diehard runs	0.577855	PASSED	0.000000	FAILED	0.833271	PASSED
diehard runs	0.104087	PASSED	0.000000	FAILED	0.139655	PASSED
diehard craps	0.991617	PASSED	0.713058	PASSED	0.000000	FAILED
diehard craps	0.370901	PASSED	0.000000	FAILED	0.000000	FAILED
marsaglia tsang gcd	0.324908	PASSED	0.000000	FAILED	0.000000	FAILED
marsaglia tsang gcd	0.142665	PASSED	0.169742	PASSED	0.000000	FAILED
sts monobit	0.623604	PASSED	0.000000	FAILED	0.000000	FAILED
sts runs	0.395052	PASSED	0.699814	PASSED	0.000000	FAILED
sts serial	0.156429	PASSED	0.000000	FAILED	0.000000	FAILED
RGB bitdist	0.716622	PASSED	0.000000	FAILED	0.000000	FAILED
RGB minimum distance	0.181222	PASSED	0.294631	PASSED	0.000000	FAILED
RGB permutations	0.804803	PASSED	0.000000	FAILED	0.838064	PASSED
RGB lagged sum	0.050637	PASSED	0.000000	FAILED	0.000000	FAILED

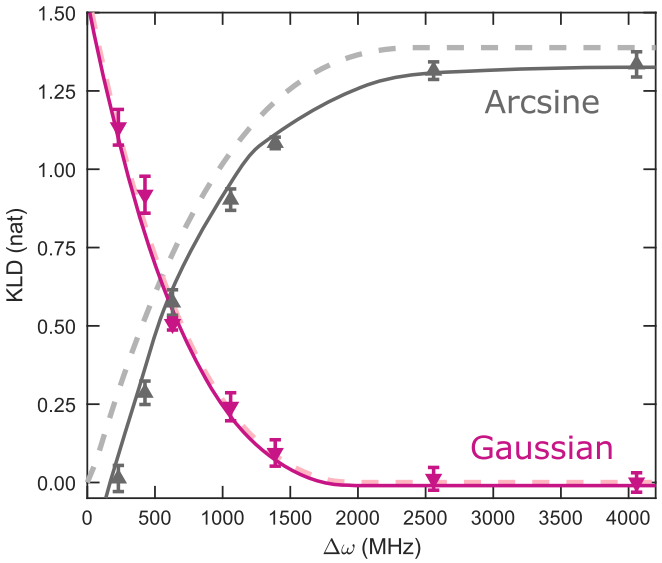

FIG. 6. Kullback-Leibler divergence as a function of the beat frequency $\Delta\omega$ when comparing the experimental probability distributions to an ideal arcsine distribution (gray dashed line and upwards triangles) and a pure Gaussian distribution (purple dashed line and downwards triangles). Dashed lines refer to theoretical predictions of a perfect system while solid lines refer to a theoretical prediction with the experimental parameters.

that a digital sampling rate of 10 GHz does not introduce high degrees of correlation in the generated bit strings. Further to random testing, it is possible to monitor the transition from quantum interference to the convolution of the two lasers by computing the Kullback-Leibler divergence (KLD) [51,53,54] (see Appendix E) on the emerging probability distributions. Figure 6 shows the KLD expressed in nat, the natural unit of information, as a function of the beat frequency $\Delta\omega$ when comparing the experimental probability distributions to both an ideal arcsine distribution (gray dashed line and upwards triangles) and a pure Gaussian distribution (purple dashed line and downwards triangles). As the LO and the SG becomes "more distinguishable," i.e., $\Delta\omega$ increases, the KLD monotonically increases from its minimum value when the divergence from a perfect arcsine distribution broadens while it decreases to a minimum when the divergence from a perfect Gaussian distribution reduces. The dashed lines in Fig. 6 represent the theoretical KLDs when comparing the experimental probability distributions to an ideal arcsine distribution (gray) and to a Gaussian distribution (purple). The data points represent the KLD computed comparing the experimental probability distributions to the experimental arcsine distribution [Fig. 4(a)] (gray upwards triangles) and the experimental Gaussian distribution [Fig. 4(d)] (purple downwards triangles). The former are shifted towards higher $\Delta\omega$ values due to experimental limitations when matching the wavelengths of the two laser sources which provides optimal quantum interference at an absolute $\Delta\omega = 206.67$ MHz rather than the theoretical $\Delta\omega = 0$. The intersection point between the two experimental KLDs ($\Delta\omega = 582.37$ MHz) defines the transition limit where the QRNG loses enough randomness to introduce high correlations in the generated numbers making the statistical random tests fail. Furthermore, the KLD analysis highlights the limiting conditions for indistinguishability between two laser sources of a heterodyne detection QRNG. The KLD also provides additional security when performing Toeplitz hashing on the raw data by providing further constraints on the generated bits.

IV. DISCUSSION

QRNGs based on phase randomization sampling between two independent lasers clearly show the ability to produce random numbers at Gb s^{-1} rates due to fast response detectors, reduced amount of optical components, and off-the-shelf devices easy to implement. They also provide the means to monitor the generation process and infer possible interference by an external party simply by reconstructing the probability distribution of the generated numbers. However, such generators lack the ability to produce numbers in real time due to the lack of distribution uniformity. Postprocessing and randomness distillation need to be performed thus reducing the overall generation rate. Here we presented a detailed analysis on how it is possible to violate the conditions for randomness generation by tampering with the system.

V. CONCLUSIONS

We presented an optical QRNG based on sampling phase randomization between two independent cw laser sources. We showed the power behind heterodyne detection and how it relates to our experiment. We analyzed how randomness generation is affected when the system is working under suboptimal conditions and an eavesdropper tampers with the experimental setup. Postprocessing and privacy amplification was required to remove biases in the generated random numbers as well as compensate for the lack of uniformity. The overall secure generation rate could be improved with faster acquisition equipment. Such QRNG could be implemented in standard QKD systems by simply replacing the SG with a fraction of the optical power from the system's source and spending its random numbers to seed the QKD protocol directly. Future work would see the implementation of a more rigorous entropy analysis involving the effects of discretization introduced by the detector [17,19,22] as well as the contribution of side information [55,56].

All data created during this research are openly available from the Heriot-Watt University data archive [57].

ACKNOWLEDGMENTS

This work was supported by the UK Engineering and Physical Sciences Research Council (EPSRC) through both Platform Grant No. EP/K015338/1 and the Quantum Communications Hub Grant No. EP/M013472/1. We thank C. R. Flegel and P. Noble for their help in setting up an early version of the experimental system and conducting initial, preliminary postprocessing analysis of a subset of the results. We also thank Dr. R. Colbeck for insightful discussions on privacy amplification and information entropy.

APPENDIX A: NIST SP 800-22 AND DIEHARDER TESTS

Tables I and II report the p-values, i.e., degree of acceptance or rejection of randomness hypothesis on the generated numbers, of all tests included in the NIST SP 800-22 and DIEHARDER suites distributed in the allowed range [0,1], as well as the resulting acceptance or rejection condition for different $\Delta\omega$ values. The level of significance α for all NIST SP 800-22 tests has been set to 0.01 which allows us to assert if a string of random values is truly random with a 99% confidence. All NIST SP 800-22 tests were performed on 128-bit strings of 10^6 bits long and all DIEHARDER tests on 128 million 32-bit numbers for statistical significance relative to a real time extraction rate of 15 Mb s^{-1}. The tests presented were performed on the raw extracted numbers, before applying any randomness distillation. The real-time generation rate was limited to only tens of Mb^{-1} due to limited USB connection speed between the computer and oscilloscope used to digitize the detector's signal. The nominal offline generation rate of 110 Gb s^{-1} is determined by multiplying the min-entropy value, the 12-bit resolution of the ADC unit, and Toeplitz hashing reduction to the 10-GHz sampling rate and assumes no speed limitations during the acquisition and postprocessing of the generated random numbers.

APPENDIX B: MAXIMIZATION OF QUANTUM PHASE FLUCTUATIONS

Optical heterodyne detection makes use of two independent sources, i.e., a local oscillator (LO) and a signal (SG), to retrieve phase and frequency information of the downmixed signals. In a semiclassical interpretation, the interference output monitored by a detector can be described as follows:

$$I_{\mathrm{D}} \propto \cos\left(\Delta\omega\, t + \Delta\phi\right), \tag{B1}$$

where $\Delta\omega$ and $\Delta\phi$ are the differences between the angular frequencies and optical phases of the LO and SG respectively. When the two sources (LO and SG) do not share any *a priori* information, $\Delta\phi$ is uniformly distributed in the range $[0, 2\pi]$. A laser source produces highly coherent photons which share a common phase whose value is dictated by the random fluctuations of the quantum process of spontaneous emission [58]. Heterodyne based QRNGs harness these quantum fluctuations as a source of randomness. However, semiconductor lasers have shown the ability to reduce such contributions when operated at high optical power levels [59]. Therefore, it is important to calibrate the system in order to minimize the predictable classical phase noise due to a system's imperfections and maximize the quantum contribution of spontaneous emission. The calibration procedure we used [60] conveniently allows us to separate the overall phase fluctuation $\Delta\phi$ as the sum of two individual components:

$$\langle \Delta\phi^{\,2} \rangle = \frac{Q}{P} + C, \tag{B2}$$

where Q and C are the quantum and classical phase fluctuations respectively and $\langle\cdot\rangle$ denotes the statistical averaging function. The quantum contribution is inversely proportional to the optical power of the laser sources while the classical noise is laser independent and collects all imperfections of the system. As a first approximation, we consider such variables as time-independent due to implementation of polarization-maintaining panda-eye fibers, internal power stabilization mechanisms for both laser sources and interferometric stability. Consequently, the variance of the intensity output I_{D} becomes

$$\left\langle I_{\mathrm{D}}^2 \right\rangle = C' P^2 + Q' P + B, \tag{B3}$$

where Q', C' are the normalized quantum and classical contributions respectively which incorporate the gain factor of the detector and B is a constant term due to the detector's background level. Information theoretic randomness requires maximization of the quantum contribution ($Q'P$) over the classical one ($C'P^2 + B$), therefore it is possible to evaluate the optimal operational power level P_{opt} which produces the highest quantum signal-to-noise ratio (QSNR) δ:

$$\delta = \frac{Q' P}{C' P^2 + B}. \tag{B4}$$

The coefficients Q', C', and B were extracted interpolating Eq. (B3) for different optical power levels P. Figure 7 shows the experimental values of the measured variance $\langle I_{\mathrm{D}}^2 \rangle$ for different optical power values P together with the interpolating curve from Eq. (B3). The plot displays the experimental data of only one laser source as the other source presents a similar trend. Table III reports the values for the extrapolated coefficients for both sources. Making use of Eq. (B3) and the interpolated values of Table III, it is possible to define an optimal power level P_{opt} for both sources which maximizes the QSNR δ (see Table IV). The internal feedback control system of the two lasers sources allows us to reduce power fluctuations to $\sim 3 \times 10^{-8}$ % of the chosen optical power also providing an extinction factor of (~ -10 dB) over the optimal working condition and (~ -6 dB) over the electrical background noise of the detector in the frequency domain.

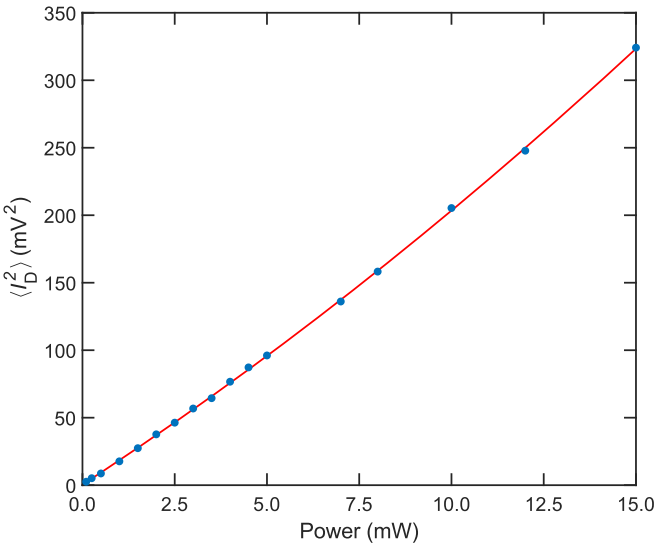

FIG. 7. Variance of intensity output $\langle I_{\mathrm{D}}^2 \rangle$ as a function of the operational optical power. Solid red line corresponds to theoretical fit using Eq. (B3) while filled blue dots correspond to the experimental values. Error bars of experimental values are less than 2.5% and covered by the plot symbols.

TABLE III. Coefficients of Eq. (B3) extrapolated from the theoretical fit for both the LO and SG.

Local oscillator (LO)			Signal (SG)		
C' (mV^2/mW^2)	Q' (mV^2/mW)	B (mV^2)	C' (mV^2/mW^2)	Q' (mV^2/mW)	B (mV^2)
0.246 ± 0.033	17.8 ± 0.4	0.39 ± 0.62	0.253 ± 0.042	17.2 ± 0.8	0.42 ± 0.39

APPENDIX C: AUTOCORRELATION ESTIMATION

Random numbers are commonly checked by testing suites, e.g., NIST SP 800-22 and DIEHARDER, in order to assess the degree of randomness they hold, however, it is also important to quantify the degree of correlation that might be introduced by an incorrect sampling mechanism during the acquisition process. The autocorrelation coefficient K allows us to perform such assessment. K is defined as follows [39]:

$$K = \frac{E[(x_i - \mu)(x_{i+m} - \mu)]}{\sigma^2}, \tag{C1}$$

where E is the expected value function, m is the bit shift, μ and σ are the mean and standard deviation of the bit string, and x_i is the ith bit value of a bit string X. Figure 8 shows the computed coefficient K for different values of $\Delta\omega$ and bit shifts. As can be seen, the autocorrelation coefficient K is the lowest for the smallest $\Delta\omega$ experimentally achievable, i.e., $\Delta\omega = 206.67$ MHz, and it increases to higher values as $\Delta\omega$ increases.

APPENDIX D: UNIVERSAL HASHING AND TOEPLITZ MATRIX

Any practical QRNG requires a postprocessing phase after obtaining raw data in order to remove almost completely the classical noise introduced by correlation with the environment [50]. The first step in doing so is to determine the amount of randomness generated by the system and the information entropy is the mathematical tool which gives this value. Of all information entropies, the min-entropy H_∞ is the one widely used for QRNGs as it provides a lower bound on the secure extractable information [47,48].

Definition D.1: The min-entropy H_∞ of a random variable X with probability distribution $\mathcal{X}$ on a uniformly distributed set $\{0, 1\}^l$ is defined as

$$H_\infty(\mathcal{X}) = -\log_2\left[\max_{\mathcal{X}\in\{0,1\}^l} \text{Prob}(X = x)\right]. \tag{D1}$$

TABLE IV. Optimal operational power levels and corresponding QSNRs for both the LO and SG. When δ is maximized the quantum contribution of spontaneous emission dominates over both the classical optical noise and intrinsic background level of the detector.

Local oscillator (LO)		Signal (SG)	
P_{opt} (mW)	$\delta(P_{opt})$	P_{opt} (mW)	$\delta(P_{opt})$
1.26	28.73	1.28	26.38

Once the min-entropy is computed, its value can be used to create a randomness extractor.

Definition D.2: An $E(k, \epsilon, l, p, s)$ extractor is a function

$$E : \{0, 1\}^l \times \{0, 1\}^p \to \{0, 1\}^s, \tag{D2}$$

with $H_\infty \geqslant z$ for a probability distribution $\mathcal{X}$ on a uniformly distributed set $\{0, 1\}^l$ such that the probability distribution $E(X, \{0, 1\}^p)$ is ϵ-close to the uniform distribution $\{0, 1\}^s$.

The extractor depends on the security parameter ϵ which defines the statistical distance between two probability distributions. The smaller this parameter is, the closer the extracted numbers are to being uniformly distributed on $\{0, 1\}$.

Now that the extractor is defined, it is possible to perform Toeplitz hashing extraction on the raw random numbers by constructing a Toeplitz random matrix and applying the concepts introduced by the Leftover Hash Lemma [3,52,61]. A Toeplitz matrix is defined as follows:

Definition D.3: A Toeplitz $n \times n$ matrix T is a matrix in which each descending diagonals are constant:

$$T_{i,j} = T_{i+1,j+1} = t_{i-j}. \tag{D3}$$

Using Eq. (D3), it is possible to define the procedure of Toeplitz hashing as follows [52]:

(1) Given a raw extracted data sample of size l, a min-entropy $H_\infty = z$, and security parameter ϵ, the length of the

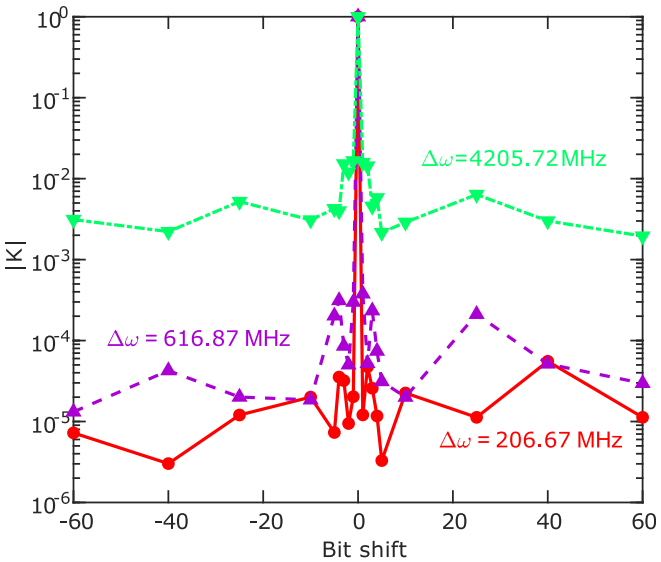

FIG. 8. Absolute value of the autocorrelation coefficient K as a function of the bit shift relative to extracted bit strings for different $\Delta\omega$ values. All values were computed from prestored raw 128-Mb strings at a fixed sampling rate of 10 GHz before randomness distillation.

Toeplitz extractor s is

$$s = \lfloor l - z + 2\log_2 \epsilon \rfloor, \tag{D4}$$

where $\lfloor \cdot \rfloor$ is the floor function.

(2) Construct a $n \times s$ Toeplitz matrix using a $2n - s - 1$ random-bit seed.

(3) Multiply the Toeplitz matrix by the raw data and extract unbiased random data of length s.

APPENDIX E: KULLBACK-LEIBLER DIVERGENCE

Entropy estimation on probability density functions associated with random variables provides a quantitative method to assessing the amount of randomness in a system. However, it fails to give information about the nature of the probability density functions, i.e., it cannot distinguish between two different probability distributions which hold the same amount of randomness. The Kullback-Leibler divergence (KLD), also called relative entropy, helps to measure the probability distance of two separate density functions [51,53,54].

Definition E.1: The Kullback-Leibler divergence KLD is a function

$$D_{\mathrm{KL}} : \mathcal{P} \times \mathcal{Q} \to \mathbb{R}, \tag{E1}$$

where $\mathcal{P}$ and $\mathcal{Q}$ are probability distributions. DKL is thus defined as

$$D_{\mathrm{KL}}(\mathcal{P}||\mathcal{Q}) = \int_{-\infty}^{\infty} p(x)\ln\left(\frac{p(x)}{q(x)}\right)dx, \tag{E2}$$

where p and q are the probability densities associated with $\mathcal{P}$ and $\mathcal{Q}$.

Following definition (E1), the KLD satisfies the following properties:

(1) It satisfies the Gibbs inequality [62],

$$D_{\mathrm{KL}}(\mathcal{P}||\mathcal{Q}) \geqslant 0.$$

(2) It is defined only for absolutely continuous probability density functions,

$$q(x) = 0 \to p(x) = 0.$$

(3) It is additive for independent probability distributions,

$$D_{\mathrm{KL}}(\mathcal{P}||\mathcal{Q}) = D_{\mathrm{KL}}(\mathcal{P}_1||\mathcal{Q}_1) + \cdots + D_{\mathrm{KL}}(\mathcal{P}_n||\mathcal{Q}_n).$$

The KLD thus measures the mutual information, i.e., mutual dependence of distributions, of two probability density functions. However, it is important to stress that, despite the KLD showing remarkable similarities with other information divergences, it is not a true metric, i.e., it does not satisfy the triangle inequality and it is not symmetric [63].

The analysis so far has been applied to a classical system where the probability density functions represent classical outcomes from a deterministic system, however, the KLD can be generalized to a quantum system by replacing the classical distributions $\mathcal{P}$ and $\mathcal{Q}$ with the corresponding density matrices $\mathbb{P}$ and $\mathbb{Q}$ which are defined on an Hilbert space $\mathcal{H}$ [64]:

$$D_{\mathrm{KL}}(\mathbb{P}||\mathbb{Q}) = \mathrm{Tr}[\mathbb{P}\ln\mathbb{P} - \ln\mathbb{Q})]. \tag{E3}$$

In a quantum framework, KLD is also implemented to measure the separability of a quantum state as an estimation of the degree of entanglement [65].

[1] B. Hayes, Am. Sci. **89**, 300 (2001).

[2] M. Herrero-Collantes and J. C. Garcia-Escartin, Rev. Mod. Phys. **89**, 015004 (2017).

[3] S. Tezuka, *Uniform Random Numbers* (Springer, New York, 1995), p. 209.

[4] Y. Dodis, D. Pointcheval, S. Ruhault, D. Vergniaud, and D. Wichs, in *Conference on Computer & Communications Security* SIGSAC 3 (ACM, New York, 2013), pp. 647–658.

[5] M. Bellare, S. Goldwasser, and D. Micciancio, *"Pseudo-Random" Number Generation within Cryptographic Algorithms: The DDS Case* (Springer, Berlin, 1997), pp. 277–291.

[6] L. Blum, M. Blum, and M. Shub, SIAM J. Comput. **15**, 364 (1986).

[7] U. V. Vazirani and V. V. Vazirani, *Efficient and Secure Pseudo-Random-Number Generation* (Springer-Verlag, Berlin, 1985), pp. 193–202.

[8] P. A. M. Dirac, *The Principles of Quantum Mechanics* (Clarendon, Oxford, 1958), p. 314.

[9] F. Xu, J. H. Shapiro, and F. N. C. Wong, Optica **3**, 1266 (2016).

[10] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, Phys. Rev. Lett. **114**, 150501 (2015).

[11] M. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, Opt. Express **18**, 13029 (2010).

[12] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **93**, 031109 (2008).

[13] M. A. Wayne, E. R. Jeffrey, G. M. Akselrod, and P. G. Kwiat, J. Mod. Opt. **56**, 516 (2009).

[14] J. G. Rarity, P. C. Owens, and P. R. Tapster, J. Mod. Opt. **41**, 2435 (1994).

[15] X. Li, A. B. Cohen, T. E. Murphy, and R. Roy, Opt. Lett. **36**, 1020 (2011).

[16] C. R. S. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, Opt. Express **18**, 23584 (2010).

[17] D. G. Marangon, G. Vallone, and P. Villoresi, Phys. Rev. Lett. **118**, 060503 (2017).

[18] J. Y. Haw, S. M. Assad, A. M. Lance, N. H. Ng, V. Sharma, P. K. Lam, and T. Symul, Phys. Rev. Appl. **3**, 054004 (2015).

[19] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, Nat. Commun. **9**, 5365 (2018).

[20] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, Nat. Photon. **4**, 711 (2010).

[21] Y. Shen, L. Tian, and H. Zou, Phys. Rev. A **81**, 063814 (2010).

[22] B. Xu, Z. Li, J. Yang, S. Wei, Q. Su, W. Huang, Y. Zhang, and H. Guo, Quantum Sci. Technol. **4**, 025013 (2019).

[23] M. J. Applegate, O. Thomas, J. F. Dynes, Z. L. Yuan, D. A. Ritchie, and A. J. Shields, Appl. Phys. Lett. **107**, 071106 (2015).

[24] W. Wei and H. Guo, Opt. Lett. **34**, 1876 (2009).

[25] M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu, and H. Zeng, Phys. Rev. A **83**, 023820 (2011).

[26] D. G. Marangon, G. Vallone, U. Zanforlin, and P. Villoresi, Quantum Sci. Technol. **1**, 015005 (2016).
[27] V. D. Preez, M. G. B. Johnson, A. Leist, and K. A. Hawick, in *International Conference on Foundations of Computer Science*, FCS4818 (CSREA, Las Vegas, Nevada, 2011), pp. 16–21.
[28] G. L. Roberts, M. Lucamarini, J. F. Dynes, S. J. Savory, Z. L. Yuan, and A. J. Shields, Quantum Sci. Technol. **3**, 045010 (2018).
[29] A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M. J. Li, D. Nolan, A. Martin, and H. Zbinden, Appl. Phys. Lett. **112**, 171108 (2018).
[30] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han, Opt. Lett. **37**, 1008 (2012).
[31] R. J. Collins, R. Amiri, M. Fujiwara, T. Honjo, K. Shimizu, K. Tamaki, M. Takeoka, E. Andersson, G. S. Buller, and M. Sasaki, Opt. Lett. **41**, 4883 (2016).
[32] R. J. Collins, R. Amiri, M. Fujiwara, T. Honjo, K. Shimizu, K. Tamaki, M. Takeoka, M. Sasaki, E. Andersson, and G. S. Buller, Sci. Rep. **7**, 1 (2017).
[33] K. Razdan and D. A. Van Baak, Am. J. Phys **70**, 1061 (2002).
[34] D. Renker and E. Lorenz, J. Instrum. **4**, P04004 (2009).
[35] R. J. Glauber, Phys. Rev. **131**, 2766 (1963).
[36] E. C. G. Sudarshan, Phys. Rev. Lett. **10**, 277 (1963).
[37] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. P. Torres, M. W. Mitchell, and V. Pruneri, Opt. Express **19**, 20665 (2011).
[38] D. G. Marangon, A. Plews, M. Lucamarini, J. F. Dynes, A. W. Sharpe, Z. Yuan, and A. J. Shields, J. Lightwave Technol. **36**, 3778 (2018).
[39] S. H. Sun and F. Xu, Phys. Rev. A **96**, 062314 (2017).
[40] Nufern, "Polarization maintaining 1550 nm telecommunication fiber" (2015), https://www.nufern.com/pam/optical_fibers/955/PM1550-XP.
[41] Mathworks, MATLAB and Statistics Toolbox Release 2017a (The MathWorks, Inc., Natick, Massachusetts, United States).
[42] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, *A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Application*, NIST special publication 800-22 Revision 1a (NIST, Gaithersburg, MD, 2010).
[43] G. Novark and E. D. Berger, in *Conference on Computer and Comm. Security*, CCS '10 (ACM, New York, 2010), pp. 573–584.
[44] M. G. A. Paris, Phys. Rev. A **53**, 2658 (1996).
[45] R. Renner and S. Wolf, in *Proc. of the International Symposium on Information Theory, 2004* (IEEE, Chicago, IL, 2004), p. 233.
[46] L. M. L. Cam and J. Neyman, *American Journal of Human Genetics* (University of California Press, Berkeley, 1967), Vol. 21, p. 690.
[47] B. Espinoza and G. Smith, Inf. Comput. **226**, 57 (2013).
[48] R. König and R. Renner, IEEE Trans. Inf. Theory **57**, 4760 (2011).
[49] C. E. Shannon, Bell Labs Tech. J. **27**, 379 (1948).
[50] C. H. Bennett, G. Brassard, and J.-M. Robert, SIAM J. Comput. **17**, 210 (1988).
[51] A. Youssef, C. Delpha, and D. Diallo, Signal Process. **120**, 266 (2016).
[52] X. Ma, F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, Phys. Rev. A **87**, 062327 (2013).
[53] J. Shlens, arXiv:1404.2000.
[54] S. Kullback and R. A. Leibler, Ann. Math. Stat. **22**, 79 (1951).
[55] Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, B. Bai, W. Zhang, W.-Z. Liu, C. Wu, X. Yuan, H. Li, W. J. Munro, Z. Wang, L. You, J. Zhang, X. Ma, J. Fan, Q. Zhang, and J.-W. Pan, Nature (London) **562**, 548 (2018).
[56] E. Knill, Y. Zhang, and H. Fu, arXiv:1806.04553.
[57] R. J. Donaldson, U. Zanforlin, R. J. Collins, and G. S. Buller, Analysis of the effects of imperfections in an optical heterodyne quantum random number generator, Heriot-Watt University, 2019, https://doi.org/10.17861/4b390eba-eca3-4fc5-92cd-796679113413.
[58] G. H. B. Thompson, *Physics of Semiconductor Laser Devices* (J. Wiley, Hoboken, NJ, 1980).
[59] C. Henry, IEEE J. Quantum Electron. **18**, 259 (1982).
[60] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, Opt. Express **20**, 12366 (2012).
[61] H. Tyagi and A. Vardy, Proc. IEEE **103**, 1781 (2015).
[62] N. Merhav, Found. Trends Commun. Inf. Theory **6**, 1 (2010).
[63] A. L. Gibbs and F. E. Su, Int. Stat. Rev. **70**, 419 (2002).
[64] V. Vedral, Rev. Mod. Phys. **74**, 197 (2002).
[65] L. Henderson and V. Vedral, Phys. Rev. Lett. **84**, 2263 (2000).